USAWC STRATEGY RESEARCH PROJECT

THE IMPLICATIONS OF NETWORK CENTRIC WARFARE

by

COLONEL ALVIN L. BAILEY
United States Army

Colonel David J. Smith
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Implications of Network Centric Warfare	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Alvin Bailey	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**27**	

ABSTRACT

AUTHOR: Colonel Alvin L. Bailey

TITLE: THE IMPLICATIONS OF NETWORK CENTRIC WARFARE

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 27 CLASSIFICATION: Unclassified

This paper will examine Network Centric Warfare, the centerpiece of Transformation. This form of warfare depends heavily on computer networks, the Internet, communications, and sensors. These areas of dependence also provide numerous vulnerabilities. This paper will focus specifically on Network Centric Warfare's vulnerabilities in terms of sensors, cyberterrorism/Electro-Magnetic Pulse (EMP) and bandwidth/frequency. The assessment of the areas listed above and the other strategic implications will lead to a conclusion as to its efficacy of Network Centric Warfare as the centerpiece of Transformation.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to personally thank Professor Patricia Pond for the countless hours she spent assisting me in the preparation, development, and linking of this document. Her patience, coaching, teaching and encouragement all led to my completion of this project. Additionally, I would like to thank LTC(P) Skip Setliff, who was bold enough and cared enough to proofread this document and provided candid comments on two separate occasions. Finally, I would like to thank my Project Advisor, Colonel Smith, whose expertise and guidance, kept me focused and allowed me to complete this project.

THE IMPLICATIONS OF NETWORK CENTRIC WARFARE

NETWORK CENTRIC WARFARE

The Army is intent on enhancing its awareness of a more complex contemporary battlefield environment by expanding the amount of information available to commanders, staffs and soldiers. To significantly enhance the ability to truly "see" the battle the Army must transform its orientation from Platform Centric Warfare to Network Centric Warfare. In other words, the Army must shift from having the best technology and information needed to fight as an aggregate of separate, individual combat entities, working on their own with the big picture seen only by the senior commanders and move to fighting as a highly networked and integrated system, where each combat element shares information with all other combat systems.

Platform Centric Warfare has historically been the manner in which warfare has been conducted over the last 80 years. The US military has fought each armed conflict since WWII using this concept. It is known as the classic American Way of War, leading to a battle of attrition. This method of warfare employs stand-alone components to provide overwhelming fire power and superior maneuver to seizing the initiative, while fixing, closing and ultimately destroying the enemy. Warfare of this type is heavily dependant on weaponry platforms to win frontal attrition-style wars. Platform centric warfare depends on a decisive battle, or series of decision battles, of a force-on-force type scenario. The tank, armored personnel carrier, helicopter, and artillery piece are all examples of conventional platforms that support platform centric warfare. Although this type warfare may employ limited digitalization, it is far from the sophistication expected in the network centric environment.

"In contrast, Network Centric Warfare is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, Network Centric Warfare translates information superiority to combat power by effectively linking knowledgeable entities in the battlespace."[1] The basic definition of Network Centric Warfare is the introduction of new technologies and the exploration of a concept of effects-based warfare is the search for greater combat efficiency. The underlying intent of this form of warfare is to reduce the amount of military power needed to complete the mission. The "bright spot" in Network Centric Warfare is the potential to generate to improved combat efficiency.[2]

The Army today is committed to transforming itself while winning the Global War on Terrorism as it is currently being waged --- in both symmetric and asymmetric environments.

For an era in which there are few conventional threats facing the country, the challenge of fighting enemies in asymmetric warfare demands new ways of thinking. Preparing for the future will require the U.S. military to rethink and develop the kind of forces and capabilities that can adapt quickly to new challenges and circumstances. The most combat engagements are being fought largely against groups of individuals. This is evident as the U.S. continues to takes down the Taliban and rolls up the Al Qaida network.[3]

The world is changing and so are our adversaries. They respect the superior combat power of the U.S. military forces and have changed their modus operandi. Current and possible future enemies appear to be fanatically committed to their political and religious ideologies. They will employ strategies to destroy U.S. resolve by attacking our homeland, killing innocent civilians, and conducting prolonged operations. Our adversaries will immerse themselves in our culture and attack at a time and place of their choosing to create maximum fear in Americans and coalition partners.[4]

This paper will address the Army's expected dependence on Network Centric Warfare to defeat the perpetrators of asymmetric warfare. This paper will also analyze network centric warfare as the replacement for platform centric warfare. Further, it will examine factors associated with sensors, bandwidth, cyberterrorist and Electro-Magnetic Pulse (EMP).

Moving the Army from Platform Centric Warfare to Network Centric Warfare is a major tenet of the Army's Transformation process. In fact, the centerpiece of the Army's Transformation is the change to Network Centric Warfare. It is important to briefly examine platform centric warfare in greater detail to set the stage for a more in-depth discussion of network centric warfare and it's potential.

PLATFORM CENTRIC WARFARE

The US Army has the most feared, sophisticated, and lethal armored vehicles in the world. The Abrams Tank and Bradley Fighting Vehicle moving at high rates of speed across the desert, brings fear to the US adversaries. The implementation of these platforms have been so successful, the enemies do not get themselves into a position where they are forced to engage US armored vehicles in the open desert. Although the Army has successfully used Platform Centric Warfare for many years, there are several problems with relying on them in future military operations. It is difficult to rapidly deploy these traditionally large platforms. The US Army has not successfully automated the platform utilizing modern technology across the entire force. Stovepiping of information presents information sharing between systems. Finally, bandwidth constraints have limited information sharing using existing technologies. These four

key issues will be examined as they reveal limitations in the current Platform Centric Warfare approach and the need to pursue an alternative conceptual framework.

DEPLOYABILITY

Present platforms are difficult to deploy quickly due to size, weight, and the sheer numbers required to accomplish most missions. Peter Drucker, a strategic management and leadership guru has observed that, "We have tried to substitute mass of purpose. We have tried to regain military potency of defense by making it gigantic, unwieldy, and complex. It never works".[5] Warfare of this type is heavily dependant on weaponry platforms to win frontal attrition-style wars. The Abrams M-1 tank weighs 70 tons and the M-2 Bradley Fighting Vehicle (armor personnel carrier) weighs 32 tons, which make both platforms difficult to move rapidly in a crisis situation. The logistical requirements for the two platforms like fuel, ammunition, and repair parts are massive. "All our combat power is useless if we cannot get it to the theater in time or maneuver it tactically," Major General James Dubik, the head of the experimental force at Fort Lewis, pointed out. "Right now our heavy forces have limited strategic deployability and our light forces have limited tactical utility. Transformation will take care of that disconnect."[6] It requires up to 650 sorties of C-5s and C-17s to move one light division. Former Chief of Staff of the Army General Shinseki said, "there is general recognition that the US Army is too heavy and will arrive too late to affect the difference."[7] The system designer's challenge is to develop systems that have similar killing power and survivability with a quarter of the weight.

ATTEMPTS TO AUTOMATE THE PLATFORMS

In platform centric warfare, the platform is the centerpiece, and all systems are developed around the platform. Jeffrey L. Hornberger, senior systems engineer at EMC's Bethesda, Maryland, office, has delved deeply into the role information storage can play in Platform Centric environment. He contents, "In a platform centric world, the platform is the major end piece and all systems were developed around the platform. Applications that were new were developed in and of themselves. There was software created for each platform, but it was not interchangeable, which is the problem. The focus was on the platform and the application, not the data that was stored on it."[8] This resulted in the stovepiping of large amounts of information in organizations. It is quite easy to install a computer and few unlinked devices into a tank, a ship, an airplane, but building a sophisticated tightly integrated network is very difficult. Another way of saying this is "platforms developed and evolved over time. They became increasing computerized, but the software that was developed was done so to improve the platform and posed little concern for inter-service interoperability or other means to leverage the digitization

effort. The system engineers were unable to completely integrate all of the platforms which led to the stovepiping of information and communications.

STOVEPIPING OF INFORMATION

"A stovepiped system is a system or platform that performs specific functions but is not necessarily interoperable with other, unrelated platforms or systems. It usually operates independently of other systems and often possesses unique nonstandard physical and functional characteristics."[9] In efficient organizations and in equipment that support these organizations information travels both vertically and horizontally. But when information can only travel up and down the chain of command of a particular platform, the platform users end up with only a portion of the total potential information. This information is limited to only that which can be collected by those particular platforms. There are some Army cultural behaviors that also lead to stovepiping of information. The traditional Army is separated by branches for each area of specialization. The Infantry, Field Artillery, Armor, and Military Intelligence, for example, design their own systems that may or may not communicate with the other branches. This is a major contributor to the stovepiping of information. If the Army has been ineffective in preventing the stovepiping of information within the Army, then it has been even more ineffective when dealing with the other Services. As a result, stovepiping of information prevent forces from sharing relevant and timely information.

"A non-networked force results in limited information flow between units and platforms. Each individual platform must rely on its own sensors, as it does not receive much external information, and can only provide limited information to the larger force. Consequently, a force wishing to dominate a large area must deploy sufficient quantities of sensors and weapons platforms to ensure coverage for situational awareness and engagement purposes. Units must continually employ screening forces and reserves to guard against unexpected, undetected enemy activity. As the enemy is located, the non-networked force must mass combat power (fires and ground combat systems) to obtain desired results against enemy units. Such massing is usually achieved by the physical concentration of systems, so that all involved can coherently act against the enemy."[10] This ultimately results in the requirement for even greater numbers of systems impacting the deployability factor previously identified.

BANDWIDTH

"Bandwidth is a term of measurement, usually expressed in bits per second, of the rate at which information moves from one electronic device to another. Many people are aware of bandwidth issues in everyday life. They are most often confronted by a shortfall in bandwidth –

awaiting retrieval of an Internet web page over phone lines and modems that are too slow. Another example of shortage of bandwidth is being told on a holiday to phone again later because no telephone lines are currently available. The lack of bandwidth can delay or obstruct communications."[11]

In Platform Centric Warfare, operations rely on the massing of combat power for effects and the lack of bandwidth influences the commander's ability to concentrate his forces. In the past, a lack of bandwidth, which limited the ability to communicate quickly and over long distances, made the use of a geographically dispersed force ineffective. Widely dispersed forces were unable to quickly respond to or mount a concentrated attack, thus they had difficulty achieving the desired effects. Limited communications (bandwidth) was one of the problems in moving and massing forces quickly over great distances.

"Recently the Congressional Budget Office (CBO), in a study prepared for the Subcommittee on Tactical Air and Land Forces of the House Committee on Armed Services, found that significant shortfalls currently exist for the Army in terms of available bandwidth. There simply is not enough bandwidth based on the present number of frequency requirements and the number of radios that exist."[12] Bandwidth is a limited resource and constant bandwidth and frequency management is required. The requirement for bandwidth has grown in every war the U.S. has fought. The bandwidth requirement has need has increased eight-fold in Central Command units alone due to the war in Afghanistan and Iraq.[13]

The four problems listed above: deployability, failed attempts at automating the platform leading to stovepiping of information, and the lack of bandwidth, are almost impossible to overcome within the platform centric force model. The major challenges listed above are driving the requirement to transition to Network Centric Warfare.

BENEFITS OF NETWORK CENTRIC WARFARE

"Modern technologies have made it possible to free the source of combat power from their physical location in the battlespace of the future allowing forces to fight effectively on the move. Network Centric Warfare uses the data network to link commanders, organizations, and combat elements. This linking provides the following: situational awareness, the ability to receive and share knowledge, better understanding of the commanders' intent. At the same time, network centric warfare generates combat power by effectively linking, warfighting elements. The network is the "glue" that enables the pieces of the military to work together. Being network centric enables people to think better, make faster decisions, and generate power better than any adversary. The information network allows soldiers to share their knowledge and direct

actions. Commanders use the network to articulate decisions and direct actions. And it is through the network that feedback can be gained, enabling commanders to interpret the effectiveness of actions that occur."[14]

Network Centric Warfare gives the US Forces the ability to reduce their battlespace footprint, which in turn reduces risk by avoiding presenting the enemy with attractive, high value targets. The ability to collect and act on information from farther and farther away and our ability to move information rapidly proves we are no longer geographically constrained. To concentrated effects no longer requires concentrated forces. "The power in network centric warfare is created by concentrating on behaviors or actions, not the platform."[15]

"Perhaps the greatest distinction between Platform Centric Warfare and Network Centric Warfare involves the linkage between sensors, shooters, and decision-makers. Platform Centric Warfare tightly links all three logically and physically, while network-centric may separate these assets and them link them in different ways. Network Centric Warfare uses data networks to link commanders, organization, and combat power for the explicit purpose of gaining situational awareness, receiving and sharing knowledge, understanding the commander's intent, and executing meaningful, coherent action. Network Centric Warfare empowers people to think better, make faster decisions, and generate power better than any adversary."[16] In a Network Centric environment forces are expected to organize themselves at the lowest level in the best manner to accomplish the mission laid out by the high commanders. This form of warfare also results in increased speed, dramatically increased awareness and knowledge.

"Network centric warfare generates combat power by effectively linking warfighting elements. The network allows the Army to move from operations based on the massing of forces to operations based on the massing of effects. Transforming from platform centrism to network centrism enables geographically dispersed forces to have such a high level of shared battle-space awareness that they can, on their own, synchronize their effort with that of other units to achieve the commanders' intent."[17]

One of the key means of massing effects is through effects-based operations (EBO). EBOs are not new and are becoming the method to conduct warfare. There are indications, as well, that will determine the way Western militaries will fight in the future. This cannot help but shape the procurement policies. One of the proponent of EBO, Major General David Deptula, director for plans and programs within the US Air Forces' Air Combat Command states that EBO is the end of strategy" not a traditional perspective of "force-on-force". The traditional as said earlier was one of attrition and if it is exemplified in the major wars of the last century. EBO

makes “parallel warfare” possible. Instead of warfare carried out in a series of operations in which targets are set one after another, ever closer to the enemy’s heartland. Parallel warfare allows you to begin where the payoff is greatest because the variety of weapons allows you to choose. Both Operation Enduring Freedom and Operation Iraqi Freedom were perfect examples of non-linear operations. Those operations served as a true test for the principle of EBO.

In an EBO campaign, “the goal of war is to get an adversary to act according to our strategic interests”, according to Major General Deptula, down to “being able to achieve one’s objectives without the adversary even knowing he’s been influenced.” It seems possible that with EBO, strategic objectives could be targeted and achieved without firing a shot- all the while the enemy would remain oblivious to the fact that they had been out maneuvered. But to do this according to Major General Deptula, will require marrying up advanced technologies (stealth and precision-guided munitions) with effects based planning. This is the result of operations of parallel warfare -- which is central to the revolution in military affairs.[18]

There are several benefits gained by units that are networked. Situation aware is one of the benefits derived from a network that is united in a particular group of units. Networked units receive information from all available sensors. Commanders are freed from dissipating combat forces throughout the battlespace solely for situation awareness and security purposes (the sensor network effectively performs this function). All weapons can potentially attack any location within range, so combat power can be applied effectively against the enemy from dispersed locations. Commanders have less need to generate large, massed formations with the intent to overwhelm the enemy. Instead, application of fires and efficiently organized ground combat forces can be focused at critical locations. Units may still have to mass fires, not the forces. They once were required to mass both to generate efficient and precise firepower that is now available. “Network Centric Warfare can be further defined as geographically dispersed forces, sharing high quality situation awareness that is collaborating and synchronizing as needed to achieve the commander's intent.”[19] Despite being more dispersed than ever before, Network Centric Warfare allow forces to function much like an integrated unit. It successfully pulls together a variety of operational forces, no matter where they are on the battlefield.

IMPROVED SENSORS, COMMUNICATIONS, AND WEAPONS

Improved sensors, communications and weapons will set the conditions for Network Centric Warfare. “Sensors are instruments that respond to a physical stimulus (such as heat, light, sound pressure, magnetism, or motion.) They collect and measure data regarding some

property of a phenomenon, object, or material. Typical sensors are cameras, radiometers and scanners, lasers, radio frequency receivers, radar systems, sonar, thermal devices, seismographs, magnetometers, gravimeters, and scintillometers. The term “Remote Sensing” indicates that the measuring device is not physically in close proximity with the phenomenon being observed.”[20]

One of the key enablers for Network Centric Warfare is the sensor. Active sensors have the ability to track and are not constrained. The new technology embedded in sensors will greatly increase their range and make them multipurpose. Future sensors will be more active and will be a shared resource. “Active radar sensors tracking objects moving in air and space can provide very accurate ranging measurements and less accurate azimuth and bearing measurements. When errors in range and bearing are factored into estimation and prediction algorithms, the net result is an error ellipsoid which describes the uncertainty associated with a track in three dimensions. In addition, when radars are employed in the operational environment, scattering and environmental effects can combine to degrade the detection and tracking capabilities of stand-alone radar sensors, particularly against stressing targets (e.g., high speed, low observables). Under operational conditions, the tracking performance of stand-alone sensors can degrade. This drop off in sensor performance can be manifested in track discontinuity, unacceptably slow track convergence, or in the worst case, inability to initiate a track.”[21]

The Tactical Warfighter Information Net – Tactical (WIN-T), now under development will provide a much improved communication system, which will also create an environment for effective Network Centric Warfare. This communications equipment will provide C4I to the tactical operations centers (TOCs) at the brigade and higher levels of command. It also will extend the range of communications, generate efficient networks, along with providing type I encryption security. It will also supply the redundancy that presently does not exist. The Joint Tactical Radio System will also assist in establishing the network at the brigade level and below.

Future Combat Systems (FCS) that are currently under development will work in conjunction with the Network Centric Warfare systems that also under development. System developers are refining the Non-Line–of–Sight–Cannon (NLOS-C) for the Field Artillery designed to provide additional firepower. It is a high-mobility 20-ton tracked platform, with dozens of new technical advancements. The new cannon will carry on board 24 projectiles, which can be fired at a rate of 6 rounds per minute and move up to 35 mph. The NLOS-C capability will work in conjunction with the Air Force and Naval assesses to provide a choice of weapon to destroy enemy targets in an Effects Based Operational environment. With

improvements in sensors, communications equipment, and indirect fire (NLOS-C) our future forces will be equipped to conduct EBO as part of Network Centric Warfare to maximize Joint Fires capability.

CHALLENGES

There are a number of challenges in adopting Network Centric Warfare. Sensors maybe deceived and exploited by clever adversaries. Cyberterrorists may target military and commercial computers and networks using conventional or EMP generating weapons. Additionally bandwidth limitations may impact on the ability to share critical information in a timely manner. These are all issued that must be resolved to maximize the potential benefits of Network Centric Warfare.

SENSOR EXPLOITATION

"Sensor exploitation is perhaps the least challenging concern in the Network Centric Warfare arena, but one which merits serious attention. Researchers at the Defense Advanced Research Projects Agency (DARPA) have identified the challenges in the future use of sensors. Sensor systems have improved considerably in the last ten years. This is the result of both automated and semi-automated technologies. But, these systems continue to produce false alarm rates that limit their operational utility. Wide-area or local area search systems produce so many false reports, that they often overtax the capabilities of subsequent precision ID sensors and sensor exploitation systems. Once a potential target is located, modern sensor systems basically lack the ability to precisely classify and identify the target. This becomes even more difficult under difficult terrain and under fire. Today, we have no technological solutions that can compete with the precision identification capability of human eyeballs behind a video screen or a sniper-scope. The speed and accuracy of precision target ID is therefore limited by the availability of humans. This capability is further limited by the inability to automatically track targets over time, create target aggregates, understand what is really going on, predict what may happen next, and use this information to proactively seek targeting opportunities. Finally, the military can't kill mobile targets if the command and control systems are too slow or too imprecise. In the present network centric environment, the military can't share sensor information if the means are not available. The means in this case includes: the available radio communications networks and the computer capabilities for integration of information and collaboration by humans."[22]

CYBERTERRORISM

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact.[23]

Cyberterrorism is another serious concern. "The ability of an adversary to prevent the military use of its computers and computer networks for any period of time, steal sensitive information, and sabotage computer systems throughout the U.S. creates great concern from military leaders."[24] "Electronics are often sensitive to extreme weather variations and shock-prone environments, therefore, expectations for massive changes in warfighting based primarily on technology and networking should be minimized. Experience on the streets of Mogadishu, the mountains of Afghanistan and the desert and urban areas of Iraq all suggest that severe weather, effective air defenses, complex terrain, and urban environments can still make combat a close fight."[25] "Adopting Network Centric Warfare with its dependence on networks which occasionally fail and are vulnerable to failures due to attacks is a reason for concern. It is important to remember that commercial computer networks are filled with actual instances of massive communication, information, security, and processing failures and it predictable that there will be more. It is one thing for web site, computer server, or a wireless home or small business to fail or be hacked; it is quite another for U.S. military forces to suffer the same degree of failure or frustration on the battlefield."[26]

"A cyberterrorist may also employ an electromagnetic bomb, or e-bomb to bring down computers or computer networks. It is a new class of weapon relies on high-power surges to provide most of the damage. It can render impotent even the most advanced digital weapons. There are relatively few items in the 21st century military inventory, which do not rely on transistors, circuit boards, and processors. E-bombs, which are known within military circles as high-power microwave (HPM) weapons that emit short but powerful burst of electromagnetic pulses that can spike into the gigawatt range but last for only microseconds. Within seconds, an e-bomb can potentially give off enough energy to blow out equipment such as a radar system, a radio, a GPS receiver, or a computer. The pulse can enter equipment like radio signals enter through the antennas or enter through unshielded wiring, circuits, and processors. The effects can range from temporary system malfunctions and lockups to outright motherboard damage.

Some attacks could cause catastrophic and permanent damages. HPM administered properly would serve as a weapon of surprise. The soldiers on the ground won't even think they have been attacked. They would think the network is just down again."[27]

BANDWIDTH

> The foremost challenge to both Platform and Network Centric Warfare is Bandwidth. Computing is the technical issue that is hidden in the shift from platform-centric to network-centric forms of warfare. Progress in the computer industry has ridden the revelation in 1979 by Intel co-founder Gordon Moore that the density of transistors on chips, and thus the price-performance of computers, doubles every 18 months. Every seven years, the performance of CPUs increases by an order of magnitude and thus computers get continually smaller, and more capable, at a remarkable rate.[28]

"As discussed previously, the CBO study, which was prepared for the Subcommittee on Tactical Air and Land Forces of the House Committee on Armed Services, examines the issue of how much bandwidth will be required to achieve the goal of digitization (the bandwidth demand) versus how much bandwidth will be provided by the Army's planned communications programs (the bandwidth supply). The service's current plans, demand will continue to exceed supply beyond 2010 – after the Army begins fielding its next generation of advanced radios and other communications equipment."[29] In the Network Centric Warfare environment the demands increase the gap between bandwidth requirements and bandwidth availability.

SOLUTIONS

Three challenges to network centric warfare are the exploitation of sensors, the threat of cyberterrorism, and the shortage of bandwidths. In order to make this new form of warfare effective these issues must be resolved. But none of the potential solutions or mitigating efforts will be easy or without high cost.

SENSOR EXPLOITATION

The sensor is one of the key enablers in Network Centric Warfare. The great concern is sensors can be and are periodically deceived. Adversaries of the US can be expected to use decoys to give false signals, incorrect locations of strong points, and hide the location of stockpiles and warehouses. As the technology improves in the ISR arena, in the optics of the UAVs, and the complexity of ground based sensors, there should be a reduction in the occurrence of sensor deception. The scientists at the Army Research Lab (ARL) are conducting extensive research to develop better sensors. There is work being done in the area of equipping sensors with the ability to effectively peel away camouflage netting to see what is

actually under or behind it. They are smaller lighter radars and other sensors that will aid in the reduction of receiving false signals. ARL is developing different and better power sources for unattended sensors, which wakeup only when a target is detected, then provide the much needed situation awareness. The researchers are working on technology to improve perimeter defense, multi-target detection, bearing estimation and target classification. They also have a goal of producing sensors that have the ability to differentiate between small arms fire, jet engines, helicopters engines, wheeled and tracked vehicles and other noises particular to the battlefield. Mastering these technologies and techniques are a few years and many dollars away. Each solution will help reduce the potential exploitation of sensors that the military is presently experiencing.

CYBERTERRORISM

Cyberterrorism is one means in which adversaries can penetrate, cripple, or destroy the network. This method of warfare has endless potential directions. As we have Brigade Combat Team in the Combat Arms, it is a worthwhile venture to develop Network Protection Teams within our structure. These teams will require sophisticated software and hardware to monitor computer networks' back doors, gateways or other vulnerable entry points in an effort to minimize or eliminate them when possible. The members of these teams must be the best and brightest that the military possess in computer science and related fields. The teams will have the responsibility to establish passwords and generate algorithms that change the passwords every five to ten minutes once the user is logged on. Another primary mission of this team would be to monitor the multi-level encryption network to detect penetration, location, and take decisive action against. This specialized team will know all of the techniques to isolate the classified networks to ensure that those without clearance are guaranteed not to have access.

The Defense Research Labs are conducting experiments in several areas on how to protect the network. There is research being conducted in the area of using Biometrics to verify the user identity, which will provide positive network access control. "Anthony J. Tether, the DARPA Director, believes that future networks will have the ability to determine whether it is under attack and take appropriate actions."[30]

Three of the basic requirements for networks are: to operate securely, to resist all attacks, and function after an EMP attack. This type of warfare may force the services to invest in EMP proof building, vans, and buildings to store spare radios, computers and other sensitive equipment. Although they are very expensive, the purchases of a few EMP harden computers and radios for critical users are a possibility that needs to be considered. "These requirements

make it clear that a new type of architecture which will include a different type of transmission media and operating system, positive network access control, node hardening and multiple paths are all necessary."[31]

BANDWIDTH

The lack of bandwidth is one of the most complex challenges to Network Centric Warfare. The ever expanding bandwidth dilemma will require continued research. The limitations imposed by the traditional rules of physics addressed to solve this problem. A potential aid in this issue is the use of computer software to compress the signals in manner that the signals are consuming less of the traditional amount of space in the frequency spectrum. All TOCs and Headquarters within cable range will be linked with fiber optic cable, which has tremendous capability and speed of transmission. As we refine the use of the wireless TOC technology, this will make available more of the spectrum and requires more research for possible solution. Reducing the amount of information that is delivered via the voice and data systems and sending it over fiber optics is a reasonable method of decreasing the amount of bandwidth consumed. The prioritization of communications traffic is a method of controlling the amount of bandwidth, but now must be strictly enforced by the leadership. High priority command information is initiated as the commander desires. All other communications that are not cleared as command and control is sent at lower priority or during non-peak times of the day and night.

Higher capacity radios that have the ability to transmit large volumes of information while consuming less of the bandwidth than the traditional radios are also worth considering. The Army must continue to leverage commercial technology to determine whether there are solutions in the commercial world to solve the bandwidth problem. The bandwidth challenge is one that had plagued the military for years, but an inadequate amount of the budget is spent in this area.

CONCLUSION

The inherit limitations of Platform Centric Warfare have made it absolutely clear that the way ahead for the US military is the path to Network Centric Warfare. There is an expectation that continued technical improvements will solve many of the issues identified above. The strategic implications are grim if the Army is not able to perfect Network Centric Warfare. Developing technical solutions or scientific breakthroughs will take money, commitment, time, and brainpower. It is critical that the Department of Defense be willing to expend the resources necessary to ensure that Network Centric Warfare is both an effective and reliable means of

operations. Proper emphasis and resourcing by all levels of the Department of Defense will ensure that Network Centric Warfare truly becomes the centerpiece of transformation.

WORD COUNT= 5585

ENDNOTES

[1] J. Garstka, John P., Stein, Frederick, and David S. Alberts, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.,: DOD C4ISR Cooperative Research Program, February 2000), 2.

[2] Edward A. Smith, Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War (Washington, D.C.: DoD Command and Control Research Program CCRP), 63.

[3] Clarence A. Robinson Jr., "Military Marches toward Agility," *Signal*, (May 2003): 17.

[4] Congress, House, Committees on Armed Services, Subcommittee on Military procurement and Military Research and Development, *Testimony on Ground Force Modernization*, 107th Cong., 11 April 2002, 2.

[5] Douglas A. Macgregor, *Transformation Under Fire: Revolutionizing How America Fights* (Westport, CN.: Praeger, 2003), 7.

[6] David Jablonsky, "Army Transformation: A Tale of Two Doctrines," *Parameters* (Autumn 2001): 43.

[7] John Sanford, "Even the Army Can Come from the Sea," *Proceedings* (December 2003): 57.

[8] Maryann Lawlor, "Military Aims to Cache in on Stored Data," *Signal* (February 2001): 3.

[9] Macgregor, 292.

[10] Jeffery R. Witsken, "Network Centric Warfare: Implications for Operational Design," (Fort Leavenworth, KS 2002), 17; available from <http://80-Stinet.dtic.mil. 650z.carlisle.army.mil/>; Internet; accessed 11 November 2003.

[11] Paul Rehmus, "The Army's Bandwidth Bottleneck," August 2003; available from <http://www.cbo.gov/showdoc.cfm:index=4500&sequence=0>; Internet; accessed 25 November 2003.

[12] Ibid.

[13] David Hughes, "PentagonTargets Bandwidth Expansion," *Aviation Week & Space Technology*, 27 January 2003, 59.

[14] "Network Support To Army Warfighters: Effective Use of Information Technology for Current and Future Battle Command Dominance (Draft)," U.S. Army Signal Center and School, Fort Gordon, GA: U.S. Army Signal Center and School, n.d.

[15] Arthur Cebrowski, "Transformation Trends," 17 February 2003; available from <http://www.cdi.org/mrp/tt-17Feb03.pdf>; Internet; accessed 14 March 2004.

[16] Jeffrey R. Witsken, "Network-Centric Warfare: Implications for Operational Design," (Fort Leavenworth, KS), 18; available from <http://80-Stinet.dtic.mil.650z.carlisle.army.mil/>; Internet; accessed 10 November 2003.

[17] Smith, 62.

[18] Nick Cook, "Effects-Based Air Operations – Cause and Effect," *Jane's Defence Weekly*, 18 June 2003.

[19] Rehmus.

[20] James Schaeffer, "What Are Sensors," 8 November 2002; available from <http://www.ipo.noaa.gov/Technology/whatAreSensorsPopUp.html>; Internet; accessed 12 November 2003.

[21] Garstka, Stein, Alberts, 141.

[22] "Future Technology Needs," available from <dtsn.darpa.mil/ixo/ wishner/info_exp.htm>; Internet; accessed 6 February 2004.

[23] Dorothy E. Denning, "Cyberterrorism," 23 May 2000; available from <http://www.cs.georgetown.edu/~denning/inforsec/cyberterror.html>; Internet; accessed 14 March 2004.

[24] Hanan Sher, "The Weapons of Inforwar," *The Jerusalem Report* (June 1998): 36, [database on-line]; available from ProQuest; accessed 20 October 2003.

[25] Macgregor, 54.

[26] Edmund C. Blash, "Network-Centric Warfare: Requires a Closer Look," *Signal* (May 2003): 57.

[27] John Knowles, "Warfare: E-Bombs; Electromagnetic Pulses on the 21st Century," *PC Magazine,* 1 July 2003, 18.

[28] Peter Layton, "Network-Centric Warfare: A Place in Our Future?" (Fairbairn, Australia: Air Power Studies Centre, 1999), 20.

[29] Rehmus.

[30] Anthony J. Tether, "Cyber-security Must Become a Feature of Network-centric Warfare," *Aviation Week & Space Technology*, 30 June 2003, 74.

[31] Alan D. Campen, "Swarming Attacks Challenge Western Way of War," *Signal*, (April 2001): 33.

BIBLIOGRAPHY

Ackerman, Robert K. "Sensors Empower Future Soldiers." *Signal* (November 2003): 23-24.

Adams, Thomas K. "Future Warfare and the Decline of Human Decisionmaking." *Parameters* (Winter 2001/2002): 57. Database on-line. Available from ProQuest. Accessed 23 January 2004.

Alberts, David S., and Richard E. Hayes. *Power to the Edge*. Command and Control Research Program Publication Series, Washington, D.C.,: DoD Command and Control Research Program CCRP, 2003.

_____. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC,: C4SISR Cooperative Research Program, 1999.

Anthony, Richard T. "Principles of Effective Multisensor Data Fusion." *Military Technology* 27 (May 2003): Vol 27, Issue 5; 29. Database on-line. Available from ProQuest. Accessed 15 October 2003.

"Army Bandwidth Shortfalls to Continue past 2010: CBO Report." Defense Daily 219 (3 September 2003): 1. Database on-line. Available from ProQuest. Accessed 15 October 2003.

"Aviation, Networking, Modularity Part of Army Focus Areas." *Potomac* (October 2003): 1. Database on-line. Available from ProQuest. Accessed 10 November 2003.

Binnendijk, Hans. *Transforming America's Military.* Washington, D.C.: University Press, 2002.

Campen, Allen D. "The First Information War (The Story of Communications, computers and intelligence systems in the Persian Gulf War)." Fairfax, V.A. AFCEA International Press, 1992.

Cebrowski, Arthur K. "Network-centric Warfare: An Emerging Military Response to the Information Age," 29 June 1999. Available from <http://www.nwc.navy.mil/pres /speeches/ccrp2_.htm>. Internet. Accessed 11 November 2003.

Chapman, Gary. "The Cutting Edge/Cyberculture; Digital Nation; Do Computers Pose a Nuclear Threat?" *The Los Angeles Times* (4 May 1998): 3. Database on-line. Available from ProQuest. Accessed 23 January 2004.

Cook, Nick, et al. "Military Priorities and Future Warfare" *Jane's Defence Weekly* (11 September 2002): 1.

Covault, Craig. "Milsatcom Fleet Bolstered as War Looms, USAF launches a Boeing Delta IV EELV Carrying a DSCS Satellite to Strengthen U.S. Military Communications." *Aviation Week & Space Technology* 158 (17 March 2003): 26. Database on-line. Available from ProQuest. Accessed 15 October 2003.

David, Hughes. "Pentagon Targets Bandwidth Expansion." *Aviation Week & Space Technology* (27 January 2003): 57. Database on-line. Available from ProQuest. Accessed 13 October 2003.

Erwin, Sandra I. "No Single Solution for Army's Infor-Tech Problems" *National Defense* 88 (July 2003): 22. Database on-line. Available from ProQuest. Accessed October 2003.

_____. "Transformation: Are the goals off target?" National Defense (November 2003): 20. Database on-line. Available from ProQuest. Accessed 23 January 2004.

Forest, Anthony. "Hi-tech terrorists turn to cyber warfare". Jane's Defence Weekly (1 September 1999): 1.

Freedman, Lawrence. "The Changing Forms of Military Conflict." *Survival* (Winter 1998/1999): 39. Database on-line. Available from ProQuest. Accessed 23 January 2004.

Fulghum, David A. "Anticipating Demand". *Aviation Week & Space Technology* 159 (22 September 2003): 56. Database on-line. Available from ProQuest. Accessed 15 October 2003.

"Future Warfare." *Military Review* (March/April 1997): 60. Database on-line. Available from ProQuest; accessed 23 January 2004.

Glidea, Kerry. "TCO Maintains Military Communications Must Adapt To Transformational Architecture*." Defense Daily* (28 February 2003): 1. Database on-line. Available from ProQuest. Accessed October 2003.

Goure, Daniel. "Location, Location, Location." *Jane's Defence Weekly* (27 February 2002): 1.

Hendren, John. "The Nation; Army Holds Its Ground in Battle With Rumsfeld; A Light-armor Program is Spared, but the service's Role in Modern Warfare Remains an Issue." *Los Angeles Times* (29 November 2002): A.1 Database on-line. Available from ProQuest. Accessed 23 January 2004.

Henry S. Kenyon. "Air Force Shapes a New Network in the Sky." *Signal* (July 2003): 23. Database on-line. Available from ProQuest. Accessed 13 October 2003.

Hershberg, Dave, and Matthew Byron. "Satellite Transponder Glut Adds Risk." *Satellite News* 25 (4 November 2002): Vol 25, Issue: 42, 1. Database on-line. Available from ProQuest. Accessed October 2003.

Hilsum, Lindsey. "Shock and Awe, Hiroshima-Style." *New Statesman* (17 March 2003): 16.

Kamran, Sistanizadeh. "What bandwidth Glut?" *Telecommunications Americans* 37 (February 2003): 16. Database on-line. Available from ProQuest. Accessed 13 October 2003.

Keeter, Hunter. "Bandwidth Tops Short List of Fleets Technology Priorities." *Defense Daily* (17 April 2003): 1. Database on-line. Available from ProQuest. Accessed 13 October 2003.

_____. "Network Centric Warfare: A Good Idea Whose Time Has Come?" *C4I News* (8 May 2002): 1. Database on-line. Available from ProQuest. Accessed 13 October 2003.

_____. "Next Internal Look to Spotlight Deployable Command and Control." *C4I News* (7 November 2002): 1. Database on-line. Available from ProQuest. Accessed 29 October 2003.

Knowles, John. "Warfare: E-Bombs; Electromagnetic Pulses on the 21st-century Battlefield." *PC Magazine* (1July 2003): 81. Database on-line. Available from ProQuest. Accessed 23 January 2004.

Macgregor, Douglas A. *Transformation Under Fire: Revolutionizing How America Fights.* Westport, CT.: Praeger, 2003.

Moore, William H. "U.S. Army transformation: The U.K. view." Military Review (May/June 2002): 68. Database on-line. Available from ProQuest. Accessed 23 January 2004.

Muellner, George K. "Battlefield 2030 Interoperability of a Myriad of Emerging Broadband Capabilities Will Become Key." *Aviation Week & Space Technology* (15 December 2003): 76. Database on-line. Available from ProQuest. Accessed 23 January 2004.

"Network Support to Army Warfighters: Effective Use of Information Technology for Current and Future Battle Command Dominance (Draft)," U.S. Army Signal Center and School, Fort Gordon, GA: U.S. Army Signal Center and School, n.d.

Roosevelt, Ann. "Aviation, Networking, Modularity Part of Army Focus Areas" *Defense Daily* (10 October 2003): 1. Database on-line. Available from ProQuest. Accessed 29 October 2003.

"Sensors Empower Future Soldiers: U.S. Army Scientists Aim to Prove That Less is More." *Signal* (November 2003): 23-26.

Smith, George. "Weapon of the week: The electromagnetic pulse bomb." *The Village Voice* (11 Feb 2003): 1. Database on-line. Available from ProQuest. Accessed 23 January 2004.

Stern, Christopher. "Pentagon Scrambles for Satellites; Military Buying Access to Commercial Vehicles to Meet War Needs." The *Washington Post* (20 March 2003): E.01. Database on-line. Available from ProQuest. Accessed October 2003.

Wall, Robert. "Pentagon Adds Weight to Future Satcom Push." *Aviation Week & Space Technology* 157 (9 September 2003): 31. Database on-line. Available from ProQuest. Accessed 29 October 2003.